# CLAIMS

What is claimed is:

1. A method comprising:

analyzing database access statements issued for an application in use;

determining accessed items and types of access for the application based on the issued database access statements for the application; and

developing a role associated with the application based on the determined accessed items and types of access, wherein the role may be used to allow a user database access when associated with the application.

2. The method of claim 1 wherein analyzing the issued database access statements comprises:

capturing the database access statements;

normalizing the database access statements; and

eliminating redundancies in the database access statements.

3. The method of claim 2 wherein the database access statements comprise Structured Query Language (SQL) queries.

4. The method of claim 1 wherein the determined accessed items and types of access include objects accessed and operations performed on the objects.

5. The method of claim 1 wherein developing a role comprises determining permissions for the application based on the determined accessed items and types of access.

6. The method of claim 1 further comprising determining which of a set of users are authorized to use the application.

7. The method of claim 1 further comprising:

detecting a user request to establish an application session;

finding the role associated with the application; and assigning the role to a user.

8. The method of claim 7 wherein detecting a user request to establish an application session comprises determining if a user is authorized to use the application.

9. The method of claim 7 further comprising:

detecting an end of the application session; and

if an end of the application session is detected, disabling the assigned role for the user.

10. An article comprising a machine-readable medium storing instructions operable to cause one or more machines to perform operations comprising:

analyzing database access statements issued for an application in use;

determining accessed items and types of access for the application based on the issued database access statements for the application; and

developing a role associated with the application based on the determined accessed items and types of access, wherein the role may be used to allow a user database access when associated the application.

11. The article of claim 10, wherein analyzing the issued database access statements comprises:

determining whether the database access statements have been captured;

normalizing the database access statements; and

eliminating redundancies in the database access statements.

12. The article of claim 10 wherein the determined accessed items and types of access include objects accessed and operations performed on the objects.

13. The article of claim 10 wherein developing a role comprises determining permissions for the application based on the determined accessed items and types of access.

14. The article of claim 10 wherein the instructions are further operable to cause one or more machines to perform operations comprising determining which of a set of users are authorized to use the application.

15. The article of claim 10 wherein the instructions are further operable to cause one or more machines to perform operations comprising:

determining whether a user request to establish an application session has been detected;

finding the role associated with the application; and

assigning the role to a user.

16. The article of claim 15 wherein detecting a user request to establish an application session comprises determining if a user is authorized to use the application.

17. The article of claim 15 wherein the instructions are further operable to cause one or more machines to perform operations comprising:

detecting an end of the application session; and

if an end of the application session is detected, disabling the assigned role for the user.

18. A database security analyzer comprising:

a communication interface operable to receive database access statements issued for an application in use;

a memory operable to store the issued database access statements; and

a processor operable to develop a role associated with the application based on the issued database access statements for the application, wherein the role may be used to allow a user database access when using the application.

19. The analyzer of claim 18 wherein developing a role comprises:

determining accessed items and types of access for an application based on the issued database access statements for the application;

determining permissions for the application based on the determined accessed items and types of access; and

developing a role associated with the application based on the determined permissions.

20. The analyzer of claim 19 wherein the determined accessed items and types of access include objects accessed and operations performed on the objects.

21. The analyzer of claim 18 wherein developing a role comprises:

determining whether issued database access statements have been captured;

normalizing the database access statements; and

eliminating redundancies in the database access statements.

22. The analyzer of claim 18 wherein the memory comprises instructions, and the processor operates according to the instructions.

23. A method comprising:

capturing the database access statements issued for one or more applications in use, wherein the database access statements comprise Structured Query Language (SQL) queries;

normalizing the issued database access statements;

eliminating redundancies in the normalized database access statements;

determining accessed items and types of access for an application based on the issued database access statements for the application, wherein the determined accessed items and types of access include objects accessed and operations performed on the objects;

determining permissions for the application based on the accessed items and types of access;

developing a role associated with the application based on the developed permissions;

determining which of a set of users are authorized to use the application;

detecting a user request to establish a session of the application;

determining if the user is authorized to use the application;

if the user is authorized to use the application, finding the role associated with the application;

assigning the role to the user;

detecting an end of the application session; and

if an end of the application session is detected, disabling the assigned role for the user.